REMARKS

Claims 1-3 (as now renumbered) and claims 4 and 6 are amended, no claims are canceled, and claims 8-9 are added; as a result, claims 1-9 (as now renumbered) are pending in this application.

No new matter has been added through the amendments to the claims. Claims 1-3 (as now renumbered) have been amended to clarify that these are claims 1, 2, and 3, as indicated on page 4 of the Office Action. Support for the additional amendments to claim 2 may be found for example, but not limited to, claim 2 as originally filed. Further, claims 1, 4, and 6 were amended merely to delete the word "high" in each of these claims.

In addition, no new matter was added through new claims 8-9. Support for new claims 8-9 may be found for example, but not limited to, claim 7 as originally filed.

In the Title

The title has been amended in order to capitalized certain words in the Title and therefore more clearly distinguish the Title from the text of the specification. The words included in the Title have not been changed.

In the Drawings

The Office Action on page 2 states,

> Figure 1 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

Applicants respectfully traverse this objection to the drawings because Applicants believe that FIG. 1 of the present application meets the requirements of MPEP § 608.02(g), which states in part,

> Figures showing the prior art are usually unnecessary and should be canceled. *Ex parte Elliott,* 1904 C.D. 103, 109 O.G. 1337 (Comm'r Pat. 1904). However, where needed to understand applicant's invention, they may be retained if designated by a legend such as "Prior Art."

Applicants do not admit that FIG. 1 is prior art. Attention is directed to the specification of the present application on page 5, lines 10-23 which states,

> Access to anyone of the broadcast signals provided by the broadcasters 1-3 requires a terminal 10 which for the subscription requiring services includes a conditional access module 10 and a secure device 12, generally provided in the form of a smart card which can be connected to the conditional access module 11. The remaining part of the terminal 10 is known as such and needs not be described in detail.
>
> In the broadcast application of fig.1, for example broadcaster 1 may be a pay television operator using a conditional access system with a number of subscribers, each subscriber having a terminal 10 with conditional access module 11 and smart card 12. Such a conditional access system may use a key hierarchy, an example of which is schematically shown in fig. 2.

Thus, Applicants believe FIG. 1 includes elements which are not prior art. Therefore, Applicants have not amended FIG. 1 to add the legend "Prior Art." If the objection to Fig. 1 is maintained, Applicants request that evidence be provided showing how all of the elements illustrated in FIG. 1 are present in the prior art. If such evidence is not provided, Applicants respectfully request withdrawal of the objection to the drawings.

In the Specification

The disclosure was objected to because of the following informalities: the specification is not arranged properly. The Office Action on page 3 references 37 C.F.R. § 1.77(b) as guidelines for Applicants' use. Applicants have amended the specification as noted above, and believe the specification as amended complies with 37 C.F.R. § 1.77(b).

No new matter has been added through the amendments to the specification. For example, with regards to the amendments made to the paragraph beginning at page 8, line 13, the amendment to change "EMM's" to "ECM's" is clearly explained throughout the application that the ECM's are encrypted/decrypted using a key P and this error also follows from a comparison with original claim 6.

The Office Action on page 4 also objected to the numbering of the claims. Applicants have renumbered the first three claims in the application as claims 1, 2, and 3 as suggested on page 4 of the Office Action, and so believe that the claims comply with 37 C.F.R. § 1.126.

Applicants therefore respectfully request withdrawal of this objection to the disclosure.

§112 Rejection of the Claims

Claims 1-7 were rejected under 35 U.S.C. § 112, second paragraph, for indefiniteness or failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Specifically, claims 1, 4, and 6 were rejected under 35 U.S.C. § 112 second paragraph, wherein the Office Action on page 5 states, "The term 'high rate' in these claims is a relative term which renders the claim indefinite." Applicants have amended claims 1, 4, and 6 by deleting the word "high" in each of claims 1, 4, and 6. Applicants submit that this amendment to claims 1, 4, and 6 overcomes the 35 U.S.C. § 112 second paragraph rejection of claims 1, 4, and 6.

Claim 2 was rejected under 35 U.S.C. § 112 second paragraph, wherein the Office Action on page 5 describes why the Examiner believes the language of claim 2 is unclear. Applicants have amended claim 2 to clarify the language of the claim, and believe that the amendments to claim 2 overcomes the 35 U.S.C. § 112 second paragraph rejection of claim 2.

Applicants respectfully request withdrawal of the § 112 rejections and reconsideration and allowance of claims 1-7.

§102 Rejection of the Claims

Claims 4-7 were rejected under 35 U.S.C. § 102(a) for anticipation by International application published under the PCT, WO 99/19822 Birdwell et al. Applicants respectfully traverse the rejection of claims 4-7.

Further, Applicants disagree that the Birdwell *et al.* patent is a § 102(a) prior art reference. Applicants believe that the Birdwell *et al.* patent is characterized as a reference under 35 U.S.C. § 102(e), and thus believes that Applicants also have the right as provided under 37 C.F.R. 1.131 to swear behind the Birdwell *et al.* patent. Therefore, Applicants do not admit that the Birdwell *et al.* patent is prior art, and reserve the right, as provided for under 37 C.F.R. 1.131, to "swear behind" the Birdwell *et al.* patent.

Regarding claims 4-7, Applicants submit that the rejection is based on a misinterpretation of the disclosure of Birdwell.

Claim 4

It is correct that Birdwell discloses a conditional access system comprising a number of subscribers, wherein each subscriber has a terminal including a conditional access module and a secure device to store entitlements. A source signal is encrypted using a first key, which first key is called a session key in Birdwell et al. (We note that in discussing Birdwell, the Examiner clearly understands the meaning of changing the first key at a higher rate as the Examiner states "Additionally, a first key within the scope of a conditional broadcast system is always changed at a high rate".)

Further, it is correct that entitlement control messages ECM's are sent to the secure devices, comprising the first key encrypted using a service key, which service key is called an authorization key in Birdwell et all. The authorization keys are distributed to the secure devices through entitlement management messages EMM's (see page 16, lines 15-17). A cracked secure device which is used in unauthorized manner is traced by finding the illicitly transferred authorization key. With this evidence the server operator can trace the authorization key to the client(s) that were assigned the authorization key (see page 17, lines 3-5).

Therefore, the Examiner is misinterpreting Birdwell et al in stating on page 7, lines 5-10 that search EMM's are sent to at least part of the terminals, wherein each search EMM comprises a different dummy key. For, in the method of Birdwell et al, a plurality (at least two) authorization keys are sent to the terminals and these authorization keys are actually used to encrypt the first keys. Therefore, in the method of Birdwell et al a series of true service or authorization keys is used, which also requires the use of ECM's comprising the first keys encrypted by each of the authorization keys of the series of authorization keys to allow the authorized subscribers to decrypt the data content. This significantly increases the complexity of the conditional access system.

In contrast to the disclosure of Birdwell et al in the method of claim 4, the ECM's comprise the first keys encrypted using just a single service key P_T during normal operation EMM's are sent to the secure devices providing the service key P_T. A cracked secure device is traced by sending a set of search EMM's, wherein each search EMM of the set comprises a different dummy key P_D and each EMM is sent to the different part of the terminals. The dummy keys P_D are not used to encrypt the first keys to obtain in ECM's.

As observed in the original application, page 3, lines 29-33 this will cause a blacked-out screen also at the legal subscribers. However, this will not lead to subscriber dissatisfaction as the cracked smart card or smart cards used by the pirate can be located in a few steps or even only one step.

Claim 5

Applicants submit that claim 5 depends from claim 3, wherein claim 3 depended from claim 1. The Office Action on page 11 indicates that claims 1-3 would be allowable if rewritten to overcome the rejections under 35 U.S.C. 112, 2nd paragraph, as set forth in the Office Action, and to include all of the limitations of the base claim and any intervening claims.

Applicants believe that claims 1-3, as amended are allowable, and so claim 5 is also allowable. Therefore, Applicants respectfully request the withdrawal of the rejection with respect to claim 5.

Claim 6

Regarding claim 6, it is noted the Examiner is correct in that Birdwell et al states that different authorization keys are distributed to different sets of terminals. However, there is no disclosure or suggestion in Birdwell et al that the source signal or the ECM's are encrypted using a multiple–key or secret-sharing cryptographic algorithm having a plurality of different decrypting keys or shares. In our opinion, Birdwell et al is silent on the cryptographic algorithm used and on the manner in which the different authorization keys are used by the different groups of terminal (authorized clients) to decrypt the sessions keys to be used to decrypt the data. Birdwell et al only discloses that the session keys are encrypted with the authorization keys and each group of cryptographic units uses one authorization key to decrypt the session keys.

Claim 7

Regarding claim 7, it is noted that Birdwell et al only discloses that if the authorized clients have been identified that received the illicitly transferred authorization key, the process narrows the population of suspect clients (page 17, line 6-9). As an example it is noted on page 17, lines 10-13 that if the clients are split into two groups, each with a different authorization

key, the process will halve the population of possible traitors with each cycle. For precise identification, the process requires a number of iterations equal to log base two of the number of clients in the population. As stated for example in the abstract, the process is repeated for the identified set of clients with a new set of decoding capabilities to successively narrow the filed of possible pirating clients, until the compromised security device is precisely pinpointed.

According to claim 7, there is no repetition of the process for an identified set of clients but in contrast the distribution of the terminals in groups of terminals is varied with each repetition of the process to trace the cracked secure device. This method is further explained on page 9, lines 1-8 of the original application.

Request for reconsideration and allowance of claims 4-7.

For at least the reasons stated above, the 35 U.S.C. § 102 rejection of claims 4-7 cannot stand. Applicants respectfully request withdrawal of the rejection, and reconsideration and allowance of claims 4-7.

§103 Rejection of the Claims

Claims 6 and 7 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Thomson Multimedia EP 0822720A1, and further in view of Birdwell et al. Applicants respectfully traverse the rejection of claims 6 and 7.

However, in view of the differences between Birdwell et al and the subject matter of claims 6 and 7, even a combination of Thomson Multimedia and Birdwell et al will not result in a method according to either claim 6 or 7.

Because the proposed combination of Thomson Multimedia and Birdwell et al fails to teach or suggest the method according to claims 6 and 7, the 35 U.S.C. § 103(a) rejection of these claims cannot stand. Applicants respectfully request withdrawal of the 35 U.S.C. § 103(a) rejection, and reconsideration and allowance of claims 6 and 7.

Allowable Subject Matter

Claims 1-3 were indicated to be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. § 112, second paragraph, set forth in the Office Action and to include all of the limitations of the base claim and any intervening claims.

For at least the reasons stated above, Applicants believe they have overcome the 35 U.S.C. § 112, second paragraph rejections of claims 1-3, and therefore respectfully request reconsideration and allowance of claims 1-3.

Reservation of Rights

Applicants do not admit that references cited under 35 U.S.C. §§ 102(a), 102(e), 103/102(a), or 103/102(e) are prior art, and reserve the right to swear behind them at a later date. Arguments presented to distinguish such references should not be construed as admissions that the references are prior art.

Regarding the further prior art mentioned by the Examiner, it is noted that US-2002/0133701 indicates a filing date of January 26, 2001, i.e. after the priority date for the present patent application. Therefore, this document is not prior art for the present patent application.

CONCLUSION

Applicants respectfully submit that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney at 408-278-4042 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

ANDREW AUGUSTINE WAJS ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
408-278-4042

Date 2/6/2006

By Mark R. Vatuone
Mark R. Vatuone
Reg. No. 53,719

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 6 day of February, 2006.

Dawn R. Shaw
Name

Dawn R Shaw
Signature